What is claimed is:

1. A method carried out by a computer when executing computer-readable program code, the method comprising:

receiving an electronic file intended for delivery from a sender to an intended recipient;

determining whether the electronic file represents a potential security risk to a computer system;

if it is determined that the electronic file represents the potential security risk, then forwarding to the intended recipient a notification indicating that the electronic file represents a potential security risk; and

receiving from the intended recipient a request to view the contents of the electronic file;

converting the electronic file from a first file format to a second file format that is different from the first file format and that prevents a computer virus in the electronic file from executing when the converted electronic file is opened by the intended recipient; and

making the converted electronic file available for viewing by the intended recipient

2. The method of claim 1, said converting occurring in response to said receiving the request to view the contents of the electronic file.

3. The method of claim 1, said converting occurring prior to said receiving the request view the contents of the electronic file.

4. A method carried out by a computer when executing computer-readable program code, the method comprising:

receiving an electronic file intended for delivery from a sender to an intended recipient;

converting the electronic file from a first file format to a second file format that is different from the first file format and that ensures that a computer virus in the electronic file is unable to harm a computer of the intended recipient; and

forwarding a uniform resource locator to the intended recipient of the electronic file, the uniform resource locator identifying at least an address of a web page containing the converted

electronic file.

5. The method of claim 4, the second file format being a HTML file format without scripts.

6. A method carried out by a computer when executing computer-readable program code, the method comprising:

receiving a certain electronic file intended for delivery from a sender to an intended recipient;

converting the certain electronic file from a first file format to a second file format that is different from the first file format and that prevents a computer virus in the certain electronic file from executing when the converted electronic file is opened by the intended recipient; and

making the converted electronic file available for viewing by the intended recipient.

7. The method of claim 6, said making the converted electronic file available for viewing comprising:

forwarding a uniform resource locator to the intended recipient of the electronic file, the uniform resource locator identifying at least an address of a web page containing the converted electronic file.

8. The method of claim 6, said making the converted electronic file available for viewing comprising:

forwarding the converted electronic file to a computer of the intended recipient.

9. The method of claim 6, said making the converted electronic file available for viewing comprising:

saving the converted electronic file in a memory that is accessible by the intended recipient.

10. The method of claim 6, further comprising:

determining whether the certain electronic file represents a potential security risk to a

computer system, said converting being in response to a determination that the certain electronic file represents the potential security risk.

11. The method of claim 10, said determining whether the certain electronic file represents the potential risk comprising:

determining if the certain electronic file contains the computer virus.

12. The method of claim 10, said determining whether the certain electronic file represents the potential risk comprising:

conducting a heuristic scan of the certain electronic file.

13. The method of claim 6, the certain electronic file being an attachment to an electronic mail sent over a network.

14. The method of claim 13, the network including the internet.

15. The method of claim 6, said receiving occurring at a desktop computer of the intended recipient.

16. The method of claim 6, said receiving occurring at a server computer.

17. The method of claim 6, said receiving occurring at a gateway computer.

18. The method of claim 6, said converting occurring at a desktop computer of the intended recipient.

19. The method of claim 6, said converting occurring at a server computer.

20. The method of claim 6, said converting occurring at a gateway computer.

21. The method of claim 6, the certain electronic file being a first electronic file, further comprising:

receiving a second electronic file intended for delivery from another sender to another

intended recipient, the second electronic file having a third file format and containing another computer virus;

converting the second electronic file to a fourth file format that is different from the third file format and that prevents the another computer virus from executing when the converted second electronic file is opened by the another intended recipient; and

making the converted second electronic file available for viewing by the another intended recipient.

22. The method of claim 6, the computer virus including a macro virus.

23. The method of claim 6, the second file format being at least one of a TXT file format, a RTF file format without embedded objects, a BMP file format, a JPEG file format, a CSV file format, a JPB file format, a GIF file format, a HTML file format without scripts, and a ASCII file format.

24. The method of claim 23, the second file format being the HTML file format without scripts.

25. The method of claim 23, the second file format being the ACSII file format file.

26. The method of claim 23, the second file format being the TXT file format.

27. The method of claim 6, the second file format being a file format having text without scripts.

28. The method of claim 6, the certain electronic file being at least one of a word processing file, a spreadsheet file, a database file, a graphics file, a presentation file, a compressed file, and a binary executable file.

29. The method of claim 6, further comprising:

determining if the first file format is one of a word processing file format type and a graphics file format type, the second file format being at least one of a TXT file format, a RTF

file format without embedded objects, and a HTML file format without scripts if it is determined that the certain file format is the word processing file format type, the second file format being at least one of a JPB file format, a BMP file format, a GIF file format, the HTML file format without scripts, and a JPEG file format if it is determined that the first file format is the graphics file format type.

30. The method of claim 6, the certain electronic file being an electronic file received by at least one of a RTP transfer protocol or a HTTP transfer protocol.

31. A method comprising:

receiving a request to view the contents of an electronic file infected with a computer virus; and

in response to the request, converting the electronic file from a first format to a second format that is different from the first file format and that prevents the computer virus from executing when the converted electronic file is opened.

32. The method of claim 31, in further response to the request, making the converted electronic file available for viewing by an entity that requested to view the contents of the certain electronic file.

33. A computer-readable medium having instructions stored thereon, the instructions when executed by a computer cause the computer to:

convert an electronic file from a first file format to a second file format, the electronic file being intended for delivery from a sender to an intended recipient, the second file format being different from the first file format and preventing a computer virus in the electronic file from executing when the converted electronic file is opened by an intended recipient of the electronic file; and

make the converted electronic file available for viewing by the intended recipient.

34. The computer-readable medium of claim 33, the certain electronic file being an attachment to an electronic mail sent over a network.

35. The computer-readable medium of claim 33, the instructions when executed by the computer further cause the computer to:

determine whether the certain electronic file represents a potential risk to security of a computer system, said converting being in response to a determination that the certain electronic file represents the potential risk.

36. The computer-readable medium of claim 35 said determining whether the certain electronic file represents the potential risk comprising:

determining if the certain electronic file contains the computer virus.

37. The computer-readable medium of claim 33, the instructions when executed by the computer further cause the computer to:

determine if the first file format is one of a word processing format type and a graphics format type, the second file format being at least one of a TXT file format, a RTF file format without embedded objects, and a HTML file format without scripts if it is determined that the first file format is the word processing file format type, the second file format being at least one of a JPB file format, a BMP file format, a GIF file format, a HTML file format without scripts, and a JPEG file format if it is determined that the first file format is the graphics file format type.

38. The computer-readable medium of claim 33, the computer virus being a macro virus.

39. The computer-readable medium of claim 33, the second file format being at least one of a TXT file format, a RTF file format without embedded objects, a BMP file format, a JPEG file format, a CSV file format, a JPB file format, a GIF file format, a HTML file format without scripts, and a ASCII file format.

40. An apparatus comprising:

a computer having means for receiving a certain electronic file intended for delivery from a sender to a intended recipient, the certain electronic file having a first file format and containing a computer virus, the computer further including means for converting the certain

electronic file from the first file format to a second file format that is different from the first file format and that prevents the computer virus from executing when the converted electronic file is opened by the intended recipient, the computer further including means for making the converted electronic file available for viewing by the intended recipient.

41. The apparatus of claim 40, said computer being a desktop computer of the intended recipient.

42. The apparatus of claim 40, said computer being a server computer of a local area network.

43. The apparatus of claim 40, said computer being a gateway computer.